绿色计算产业联盟

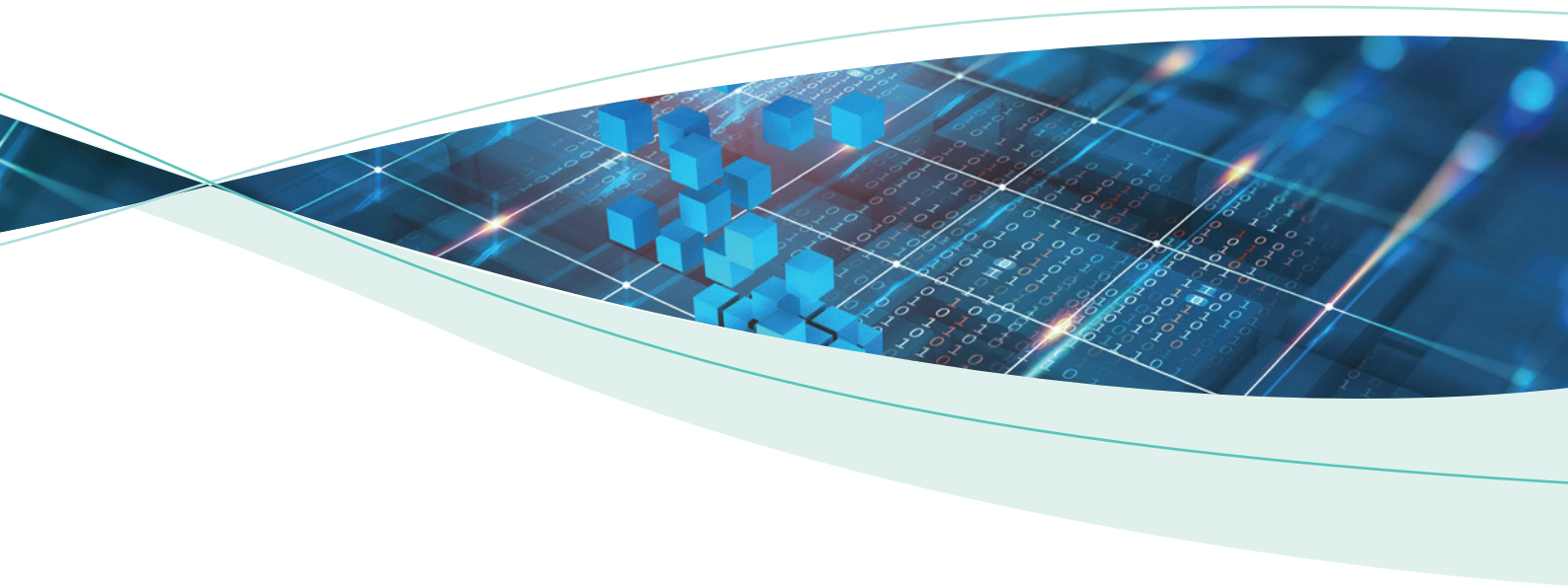
二零年十一月

OpenGCC

绿色计算服务器机密计算安全白皮书

OpenGCC ESI arm 中国 HUAWEI AMPERE PHYTIUM 飞腾 Baidu 百度

目录 CONTENTS



01 机密计算概述

1.1 机密计算概念与范围

近年来随着网络与计算业务的快速发展，越来越多的关键性服务和高价值数据被迁移到了云端和边缘，与传统的本地数据保护策略不同，对数据的保护也变得更加复杂。当前的数据保护通常作用于静态存储或网络传输状态的数据。但是当数据正在被使用时，仍然存在风险，这也是数据保护中最具挑战性的一个步骤。另外从欧盟 GDPR 到我国个人信息保护法，数据隐私监管保护的范围愈加扩大，力度日益增强，对关键数据和业务进行安全保护，是合规遵从的关键因素。

目前安全领域重要的一项技术进展名为机密计算（Confidential Computing）。机密计算可以保护使用中数据的安全性，其应用场景非常广泛，特别是在云计算领域，常见的应用有基于 Enclave 的加密数据分析、版权保护、基因数据处理、密钥保护、密钥管理系统、隐私保护的机器学习、以及保密数据库等。其他如区块链隐私计算、区块链、可信 AI、隐私边缘计算等都可以构建在机密计算技术基础上，以更好的服务应用场景。机密计算技术是一种创新的数据隔离和加密处理技术，它可以从服务器芯片硬件层保障即使 OS kernel、Hypervisor、甚至 BIOS 等特权软件都已经遭到破坏甚至本来就是恶意的情况下，敏感数据和代码依然能安全无虞，确保重要应用数据和代码的机密性和完整性，为关键业务提供易用、安全、集群化的绿色计算环境，对绿色计算产业的发展具有重要意义。

2019 年 8 月，全球主要科技公司 Alibaba、Arm, Baidu、IBM、Intel、Google Cloud、Microsoft、Red Hat、 华为等宣布成立机密计算联盟（Confidential Computing Consortium），专注于保护使用中的数据，推广机密计算在行业中的应用。机密计算在国际机密计算联盟 CCC 中，定义为：机密计算是通过在基于硬件的可信执行环境中执行计算来保护使用中的数据的一种技术 [1]。

根据 Gartner 报告 [2]，机密计算是将基于 CPU 的硬件技术与云服务提供商 CSP 虚拟机映像以及软件工具相结合，使能云租户能够创建完全隔离的可信执行环境（称为飞地 enclaves）。因为它们提供了对使用中数据的一种加密形式，主机操作系统和云提供商管理员都看不到这些飞地 enclaves 内的敏感信息。

机密计算并不仅限于云计算用途，它可以适用于任何场合，包括本地服务器、网关、IoT 设备、边缘部署、用户设备等。机密计算也不限于任何特定处理器的可信执行环境，它可能运行在 GPU 或网卡中。尽管加密是最常用的技术，机

密计算也不仅限于使用加密的解决方案。同理，机密计算并不是保护使用中的数据的唯一技术。

为了保护数据使用中的安全，有两类技术，一类是基于密码算法的，如隐私计算（Privacy-Preserving Computation）等，另一类是基于硬件的，即所谓的机密计算（Confidential computing）。隐私计算与机密计算不同，隐私计算主要以密码学计算为信任根，包括同态加密、多方计算等，如图 1 所示。隐私计算在整个数据处理过程中保持密态，更加侧重于保护用户的隐私，其运行效率较慢，目前商用还有待进一步提高性能。在图 1 中，强调基于硬件实现可信执行环境的机密计算与可信计算（TPM\TCM\TPCM）也有一定的区别。可信计算的主要特征是主机可靠性和信任链验证机制，通过容错算法、故障诊查实现计算机部件的冗余备份和故障切换，以及通过主程序调用芯片实现被动或主动度量。此外，在国际 CCC 联盟中，也认为内存加密不是必须的，加密只是其中一种实现方式，采用隔离等访问控制也是一种保护数据机密性的一种方式。

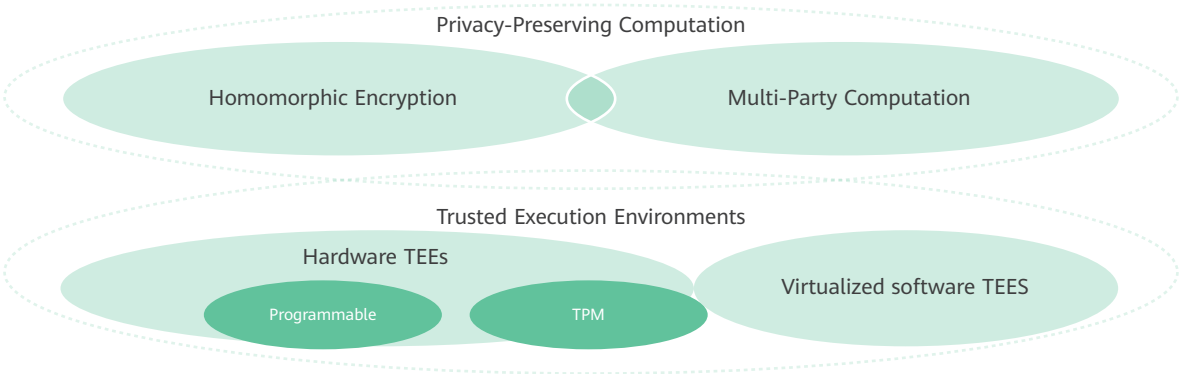


图 1 机密计算概念范畴　　（Source[1]：ccc，2020）

1.2 机密计算重要性和价值

随着大数据的进一步发展，重视数据隐私和安全已经成为世界性的趋势，各国都在加强对数据安全和隐私的保护，我国在个人信息保护方面已经开展了较长时间的工作。2016 年 11 月 7 日，全国人大常委会通过的《中华人民共和国网络安全法》中明确了对个人信息收集、使用及保护的要求，并规定了个人对其个人信息进行更正或删除的权利。

2019 年，中央网信办发布了《数据安全管理办法（征求意见稿）》，向社会公开征求意见，明确了个人信息和重要数据的收集、处理、使用和安全监督管理的相关标准和规范。这些法律法规在促进数据的合规使用、保障个人隐私和数据安全等方面发挥不可或缺的重要作用，但在客观上也不可避免地增加数据流通的成本、降低数据综合利用的效率。2020 年 7 月 3 日，《中华人民共和国数据安全法（草案）》全文在中国人大网公开征求意见。草案内容共 7 章 51 条，提出国家将对数据实行分级分类保护、开展数据活动必须履行数据安全保护义务承担社会责任等，主要内容包括：确立数据分级分类管理以及风险评估、监测预警和应急处置等数据安全管理各项基本制度；明确开展数据活动的组织、个人的数据安全保护义务，落实数据安全保护责任；坚持安全与发展并重，规定支持促进数据安全与

发展的措施；建立保障政务数据安全和推动政务数据开放的制度措施。

2020 年 10 月 21 日,《中华人民共和国个人信息保护法（草案）》在中国人大网公布，公开征求社会公众意见，本法与《网络安全法》和《数据安全法（草案）》相衔接，共同促进数字经济健康发展。

数据已经成为国家基础性战略资源，并日益对全球生产、流通、分配、消费活动以及国家治理能力产生重要影响，数据已经明确被作为一种新型生产要素写入国家指导文件之中，与土地、劳动力、资本、技术等传统要素并列为要素之一。在大数据生产要素的流通过程中，数据安全以及隐私的保护已经成为了必要条件。如何兼顾数据开放共享和数据隐私安全，在保障安全的前提下，不因噎废食，不对大数据价值的挖掘利用造成过分的负面影响，是当前全世界在数据治理中面临的共同课题。

大数据战略已上升为国家战略高度，各部委从战略规划、技术能力提升、应用与管理三个层面积极落实推进大数据发展政策。自 2016 年以来，习总书记和党中央反复提及大数据在治国理政中的重要地位，明确要求 " 实施国家大数据战略加快建设数字中国 "，我国大数据建设迎来新局面。目前，大数据发展的一个挑战就是数据安全与隐私问题，用户可能不愿意上传敏感数据到云端，担心个人信息或重要数据被泄露，有的企业不愿意进行大数据共享和交易，数据也不愿意交给其他机构进行人工智能的训练或提取。

当前的数据保护通常作用于静态存储或网络传输状态的数据，解决不了的个人信息或者重要业务数据使用阶段的安全问题和风险，而机密计算从保护使用中的数据安全角度，提供内存数据保护、数据安全存储、敏感数据处理与监测的安全服务，进一步保证应用业务使用中的数据安全，为国家大数据战略保驾护航。

机密计算涉及跨越大数据、云计算和芯片安全等纵深的安全防护体系，增强服务器、网络、应用中的重要数据识别和抵抗各种安全威胁的能力，为绿色计算的发展构建安全可信环境，加速并保障绿色计算产业发展。

1.3 绿色计算机密计算技术框架

机密计算在具体实现时实际上是通过基于硬件和软件的能力，构建和运行提供一种与不可信环境隔离的 TEE（可信执行环境）并保障其机密性，正是这种隔离和可信验证机制使得机密计算成为可能。常见的技术代表包括基于硬件能力实现的 Intel SGX，AMD SEV，Arm TrustZone 等，或者虚拟化技术实现的微软的 VSM 等。

绿色计算服务器主要基于硬件隔离机制，能让开发者构建具有可移植性的应用，并轻易部署到不同的应用侧及 TEE 侧。它提供了对于 TA（Trusted Application）的封装，以方便的运行于 TEE 内部，关键的数据和代码在 TA 中存储和运行。在应用侧（非可信环境），提供一个 SDK，和 TA 交互。应用只需要调用 SDK 的接口，就可以和 TA 通信。

绿色计算服务器机密计算在每层提供了模型化的开放接口，实现了架构的全层次开放；通过纵向从芯片到安全 OS、软件接口服务、安全应用与服务等，实现业务的全流程、全生命周期的数据安全服务。

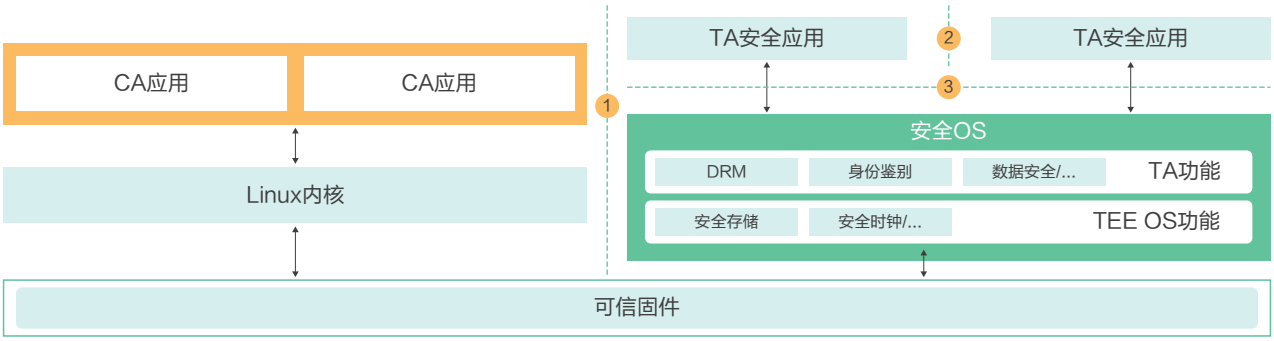


图 2 绿色计算服务器机密计算技术框架图

绿色计算服务器机密计算整体技术框架图如图 2 所示，分为三个层次：

1. 利用 Arm Trustzone，实现 TA 隔离区对 CA 机密。利用 Enclave，提供 CA 安全接口，实现各 OS 平台已有的安全能力向应用层 CA 提供统一接口的安全能力，兼容统一 Intel SGX，Arm Trustzone，RISC-V 社区 keystone 等框架，屏蔽 OS 差异与 TEE 环境。

2. TA 与 TA 之间不可见，互相之间隔离，保障数据机密性、数据完整性以及代码完整性。利用可信执行环境，遵循 Global Platform TEE 标准，屏蔽 TA 应用之间的逃逸与渗透。

3. 利用内存加密，实现底层芯片对 TA 内部的数据机密性、数据完整性以及代码完整性，同时根据应用场景提供代码完整性、安全启动、验证度量等功能。依托统一安全运行环境层，实现 TA 和 TEE OS 之间的安全应用接口标准化，屏蔽设备底层芯片的差异与 TA 内部的数据。

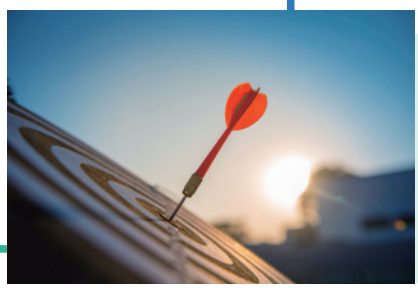
1.4 白皮书的内容和范畴

本白皮书描述了服务器机密计算的参考架构、安全需求、关键技术、标准以及典型应用场景，为开发者提供一个在服务器可信执行环境 TEE 中执行安全的开发和应用指南。

本白皮书以推动机密计算安全的产业共识为目标，为相关产业生态链构建和使用相关能力提供参考借鉴。

本白皮书定位及价值是从保护使用中的数据角度出发，建立基于 Arm 体系的机密计算统一框架和标准，指导 Arm 体系机密计算产业实践落地，做大产业空间：

- 在机密计算实现的过程中给出技术参考架构及关键技术点，推动机密计算安全技术的产业共识，牵引机密计算产业落地的技术方向；
- 指导解决绿色计算服务器产品在开发过程中存在的互联互通与适配问题，帮助产业链生态玩家找到自己在机密计算产业中的位置、应用场景、以及上下游生态的合作协同。



02 安全挑战及机密计算需求

2.1 数据安全与隐私挑战

随着计算从内部部署转移到公共云和边缘，对数据的保护变得更加复杂。用户安装的应用程序一方面要尽可能安全，需要确保所有层都不是恶意的或不受影响的，即使这没问题，仍然需要信任云服务提供商实际上正在运行主机的系统。虽然有许多技术可以解决这些层次的安全问题，例如从受信任的信誉良好的组织采购各个层次软件，但最终恶意行为者可以利用的攻击面依然很大，用户不仅需要信任云服务提供商及其员工，而且还需要信任他们系统上运行的所有软件，这已经成为云计算高安全需求的一个重大安全挑战。

基于硬件的可信执行环境 TEEs 目前在云计算环境已成为趋势，但是 TEEs 技术在高安全、复杂信任场景下的应用，目前还需要进一步解决安全和效率问题。

随着新基建不断深入，Arm 架构以及国产服务器等领域逐渐被市场关注，实现绿色计算服务器机密计算功能已经成为迫切的现实需求，芯片厂商可以抓住机遇，以更高效和简洁的使用 TEE 资源提供机密计算服务，为 Arm 服务器芯片开辟新赛道，借助服务器进入电信、安平、金融等有较高要求的行业，扩大 Arm 服务器芯片的市场占有率。目前，数据利用、合理开放与共享等方面存在安全和隐私方面的挑战及需求如下。

2.1.1 数据隐私与数据价值挖掘存在巨大矛盾

一方面，缺乏数据的数据分析公司对数据共享开放需求十分迫切，迫切得到海量、高质量的数据资源来进行分析和挖掘，另一方面，拥有大量数据的单位如政府、金融等行业，由于国家数据安全法律法规限制，不敢、不愿、不能完全地开放数据。因此数据隐私与数据价值挖掘存在巨大矛盾，现有粗暴地集中数据来使用的模式面临重大挑战，亟需一种兼顾隐私保护、数据安全和数据流动利用的新技术来平衡该矛盾。

2.1.2 数据开放共享困难

当前数据开放使用场景由“数据使用者通常是数据所有者”向“数据使用者和所有者可能不是同一方”转变。现有数据开放模式如“黑屋子”线下模式和 API 模式都局限于数据源本地，数据分析、部署模型、调试算法等都需要去数据源本地，人力、精力投入巨大。此外，上述开放模式只能小范围数据开放，无法充分发挥数据价值。另外，采用防火墙等传统边界防护手段来防范外部攻击，一旦数据边界被攻破，将无法保障数据安全。采用对数据的访问控制、审计以及脱敏来解决数据安全问题，无法保障数据被调用后的安全问题，且脱敏后的数据价值被大大降低。因此，如何合法合规地解决数据开放问题，如何既保证数据隐私又可充分挖掘数据价值，保证数据所有权和使用权分离，是大数据时代面临的核心问题。

2.1.3 数据访问权限混乱

单位内数据源众多，数据开放接口繁多，不可避免存在着数据授权粒度粗、数据访问权限过大、内部操作权限滥用等诸多问题。同时，企业缺乏有效的敏感数据的控制保护机制，如果不及时解决，数据的安全性难以充分保证。

2.1.4 数据操作缺乏审计

目前企业对数据的不当授权和第三方滥用，缺乏有效的监管审计机制。在数据应用过程中，每天都有不同的用户对数据进行各种操作，无法得知某个用户对数据具体做了什么操作、是否有违规和误操作，难以追溯审计定责。

2.1.5 流出结果缺乏审核

数据使用方完成数据操作后带走结果，缺乏严格审核，导致数据流出过程不可控的。数据使用方在带走结果的过程中，有意或无意地会夹带一些隐私数据，数据一旦流出管理边界，就会被二次分发，造成敏感数据泄露事件。

2.1.6 安全与隐私保护立法趋严

我国在个人信息保护方面也开展了较长时间的工作，针对互联网环境下的个人信息保护，制定了《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《电信和互联网用户个人信息保护规定》、《全国人民代表大会常务委员会关于维护互联网安全的决定》和《消费者权益保护法》等相关法律文件。《中华人民共和国网络安全法》、《数据安全法（草案）》、《个人信息保护法（草案）》中明确了对用户数据、个人信息等收集、使用及保护的要求。2019 年 5 月，中央网信办发布了《数据安全管理办法（征求意见稿）》，明确了个人信息和重要数据的收集、处理、使用和安全监督管理的相关标准和规范。2019 年 12 月 1 日，《网络安全等级保护制度 2.0》相关标准正式实施；2020 年 1 月 1 日，《中华人民共和国密码法》正式实施，这些法律规范均要求保证数据的合规使用、保障个人隐私和数据安全，立法趋严。

2.2 机密计算安全的需求特征

机密计算的安全需求包括数据机密性、数据完整性、代码完整性、代码机密性、安全启动、可编程性、可验证性、可恢复性以及防侧信道攻击等 [3]。其中，数据机密性、数据完整性、代码完整性是必备属性，其它的安全需求特征可选。

数据机密性保障未经授权的实体不能查看正在 TEE 中使用中的数据。数据完整性即未经授权的实体不能在 TEE 内部添加、删除或更改使用中的数据。代码完整性即未经授权的实体不能添加、删除或更改在 TEE 中执行的代码。

代码机密性即 TEE 会保护正在使用中的代码免遭未经授权的实体查看，例如保护一个敏感的算法。安全启动即 TEE 可执行授权或验证检查启动请求的进程，并可能拒绝未经认证或授权的启动进程。可编程性指 TEE 可以用代码编程，而有些 TEE 可能只支持有限的操作，TEE 甚至可能只由当时生产时固定的代码组成。可验证性是 TEE 能够提供其起源和现状的证据或度量，以便另一方能够对证据进行核实。可恢复性即某些 TEE 可能提供从不合规或潜在风险中恢复的机制。防侧信道攻击即阻止攻击者通过利用 TEE 本身的体系结构推断出 TEE 内部的数据或者操作信息。

此外，由于机密计算中处理的数据量大，要求相关的安全服务突破吞吐量、延迟和交互次数限制，可采用的解决方案包括支持轻量级加密协议，多策略的访问控制、多秘钥加密方案等。由于机密计算的硬件能力和软件类型呈多样化，安全需求也呈多样化，要求相关安全服务能够突破对复杂 TEE 类型、数据等管理能力的限制，即机密计算对不同数据类型、设备安全机制的配置应具有透明性，能够根据应用场景满足实时性应用和服务的需求。

绿色计算服务器机密计算是针对隐私保护与数据价值挖掘之间存在巨大矛盾这一痛点问题，结合各类法律法规对数据安全开放的要求，秉承“数据不动程序动”、“数据可用不可见”的安全理念，支持多种数据源，支持对数据访问权限严格控制，支持对所有数据操作留痕审计，支持行为风险分析和识别，具备数据访问申请与授权体系和输出结果申报与审核机制，实现数据所有权和使用权分离。

机密计算的目标是帮助用户突破“不敢”、“不愿”、“不能”共享数据的困境，通过合法合规安全地对外开放数据，既保证数据安全，又能充分发挥数据的最大价值，助推企业数据业务的快速发展，助力企业数据开放运营，实现社会价值和经济价值。

2.3 机密计算安全的边界

区别于存储安全和传输安全，机密计算安全具备数据机密性、数据完整性、代码完整性、代码机密性、安全启动、可编程性、可验证性、可恢复性以及防侧信道攻击等特征。因此只有考虑了上述数据机密性、数据完整性、代码完整性等必备需求特征，同时根据应用场景提供代码完整性、安全启动、验证度量等扩展功能，且面向使用中的数据安全的计算才属于机密计算安全的边界范畴。

03 机密计算安全参考架构

3.1 多视图呈现

1）安全功能视图

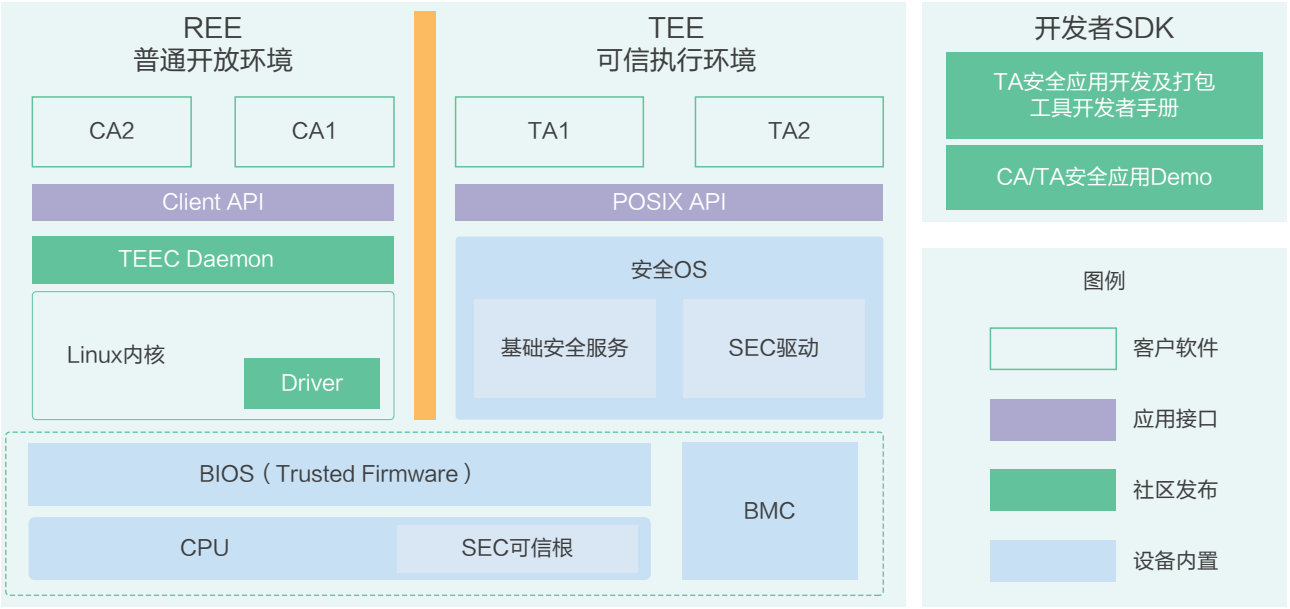


图 3 机密计算安全功能视图

功能视图侧重于系统中的功能组件、它们之间的相互关系和结构、它们之间的接口和交互，以及系统与支持该系统活动的外部元素的关系和交互。系统和组件架构师、开发人员和集成商特别关注这些问题。

在机密计算安全功能视图 3 中，主要分为 REE 普通开发环境、TEE 可信执行环境以及底层的 BIOS、BMC 等。服务器出厂预置 BIOS、BMC、安全 OS，此外可以通过社区开源开发者 SDK 与 TA 开发工具与文档、安全应用的 demo，如远程证明、TA 迁移等，以简化应用开发，同时开源 REE OS 补丁，例如：TEEC Daemon、Driver 等。

开发者用户可以基于 TrustZone 标准接口开发 REE 侧 CA 及 TEE 侧 TA，北向接口一致，应用基本兼容主流 TrustZone 安全 OS，已有 TrustZone 安全应用可快速跨 Arm 平台及安全 OS 迁移。用户可以利用 Client API 以及系统 POSIX API 进行开发，其中 POSIX 表示可移植操作系统接口（Portable Operating System Interface of UNIX，缩写为 POSIX），POSIX 标准定义了操作系统应该为应用程序提供的接口标准。POSIX 标准意在期望获得源代码级别的软件可移植性，即为一个 POSIX 兼容的操作系统编写的程序，应该可以在任何其它的 POSIX 操作系统上编译执行。

2）角色视图

机密计算的关键角色概念包含三种：机密计算服务使用方，机密计算参与方，协调方。具体的角色视图如图 4 所示。

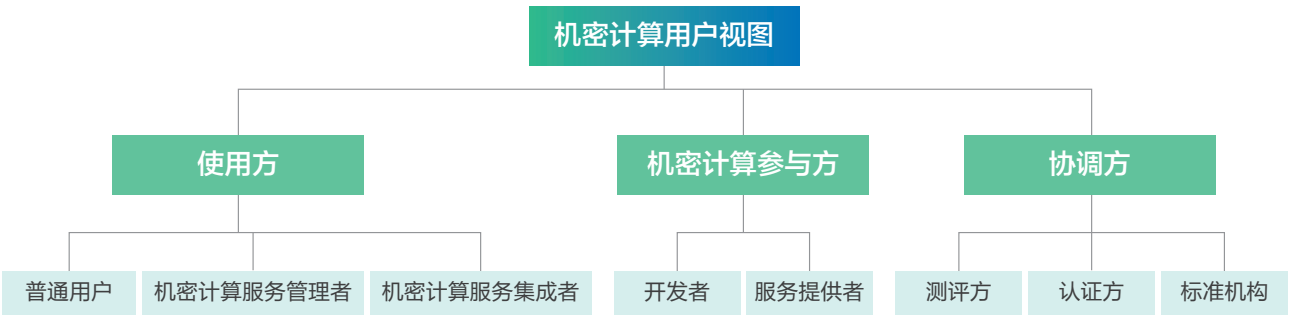


图 4 机密计算角色视图

» 机密计算服务使用方

机密计算服务使用方可以是自然人或代表该自然人的实体，是使用服务的用户。在机密计算参考架构中，服务使用方还被细分为 3 个子角色：机密计算普通用户、机密计算服务管理者、机密计算服务集成者。他们的主要活动包括：

a 使用安全加密计算协议、算法等；
b 对用户的身份、角色、权限进行管理，对计算数据进行管理等；
c 集成机密计算服务、数据融合与安全共享等。

» 机密计算参与方

机密计算参与方主要参与机密计算计算，并对其他参与方或用户提供服务。其子角色包括机密计算开发者和服务提供者。他们的主要活动包括：

a 开发或者提供安全加密计算协议、数据加密等；
b 对用户提供的服务清单、服务接入、服务规划等；
c 服务包括生产、发布、管理数据（包括但不限于存储方式、使用方式、加密方式）、使用数据等。

» 机密计算协调方

机密计算协调方为参与方的活动提供支撑或辅助功能，其子角色包括测评方、认证方和标准机构。机密计算协调方宜为第三方机构或组织。协调方活动随合作方类型及与服务提供方和客户之间关系的不同而变化。他们的主要活动包括：

a 对提供机密计算服务的产品进行测试工作等；
b 对提供机密计算服务的产品或组织履行认证职责等；
c 承担部分机密计算架构管理、接口互联互通的标准协调管理等。

3.2 机密计算关键技术

3.2.1 机密计算安全技术

在机密计算解决方案和参考实现过程中，涉及的关键技术主要有：

1 安全域隔离

安全域隔离是指在服务器 CPU 的不同安全域之间虚拟隔离资源，控制安全资源调配，实现不同业务场景下的安全隔离。隔离技术需要通过对不同安全域之间通信的数据完整校验、数据的安全检查及建立安全连接的方式来实现不同业务通信单元之间有效的安全隔离。

2 完整性保护

完整性保护是指对机密计算数据进行完整性检查和验证，保障数据的完整性，进而保证服务器运行在预期的状态，因此需要 CPU 的安全验证以及轻量级的可信链传递及度量方法，保证度量结果验证的时效性和准确性，实现系统或应用的安全启动和可信启动。

3 虚拟化安全

在机密计算环境下，虚拟化安全是指基于虚拟化技术，实现对服务器的虚拟化隔离和安全增强。相较传统云服务器，需要提供低底噪、轻量级的虚拟化框架；需要基于虚拟化框架构建低时延、确定性的 OS 间安全隔离机制和 OS 内安全增强机制；需要增强 hypervisor 本身的安全保护，消减虚拟化攻击窗口。

4 安全 OS

在机密计算环境下，安全 OS 是指 TA 层依赖的安全操作系统，支持额外的硬件安全特性（如 TPM、SGX enclave、TrustZone 等）等。需要提供协同的 OS 恶意代码检测和防范机制、统一的开放端口和 API 安全、应用程序的强安全隔离、可信执行环境的支持等关键技术，在保证操作系统自身的完整性和可信性的基础之上，保证其上运行的各类应用程序和数据的机密性和完整性。

5 安全监测

安全监测是指持续监控服务器是否存在缓慢或故障组件，或者受到侧信道攻击等，并在故障、中断等情况下通知安全管理员。设备受到攻击后，也有可能会发起针对特定目标的分布式拒绝服务攻击 DDoS。因此，进行有效的安全监测是机密计算安全的重要组成部分。通过监测 CPU 性能，实时监测链接的传输内容，能够及时发现违规行为，防止设备受到网络攻击。

6 数据安全

数据安全保障数据在 CPU 存储以及在复杂异构的环境中传输的安全性，同时根据业务需求随时被用户或系统查看和使用。亟待新的数据安全治理理念，提供轻量级数据加密、数据安全存储、敏感数据处理和敏感数据监测等关键技术能力，保障数据的产生、采集、流转、存储、处理、使用、分享、销毁等环节的全生命周期安全，涵盖对数据完整性、保密性和可用性的考量。

7 数据隐私保护

针对机密计算数据脱敏防护薄弱、获取数据敏感程度高、应用场景具有强隐私性等特点，面向机密计算隐私数据泄露、篡改等安全风险，突破机密计算轻量级加密、隐私保护数据聚合、基于差分隐私的数据保护等技术难点，实现机密计算设备共享数据、采集数据、位置隐私数据等数据的隐私保护。

8 权限和访问控制

权限与访问控制定义和管理用户的访问权限，通过某种控制方式明确的准许或限制用户访问系统资源或获取操作权限的能力及范围，控制用户对系统的功能使用和数据访问权限。需要提供轻量级的最小授权安全模型（如白名单技术），去中心化、分布式的多域访问控制策略，支持快速认证和动态授权的机制等关键技术，从而保证合法用户安全可靠的访问系统资源并获取相应的操作权限，同时限制非法用户的访问。

9 渗透测试

渗透测试是从攻击者角度，对现有系统进行脆弱性发掘与利用，以达到系统风险评估的目的。渗透测试是脆弱性评估的一种方式。需要在渗透测试阶段制定具有保障可控性和完整性的测试方案，保证测试人员了解整个测试过程以及由此产生的结果，力求全面，同时面向服务器上可能运行的定制操作系统、调用不安全第三方软件或组件等安全风险，突破自动化操作系统安全策略配置、自动化的远程代码升级和更新、自动化的入侵检测等技术难点，形成代码完整性验证以及代码卸载、启动和运行时恶意代码检测与防范等能力，实现机密计算全生命周期的恶意代码检测与防范。

10 响应与恢复

响应与恢复是指服务器被入侵之后，做出反应和恢复的过程。恢复过程中，通常需要解决两个问题：一是被入侵所造成的影响评估和系统的重建，二是恰当的外部措施的采取。其中外部措施的采取，又直接与评估和重建过程中所形成的结论相关。需要产生快速的务响应，满足行业在实时业务、应用智能、安全与隐私保护等方面的基本需求。因此，需要做好服务器应急响应准备工作，制定应急响应预案并演练，能够及时发现机密计算安全事件并做出处置，阻止或减小事件影响。

3.2.2 基于 TrustZone TEE 机密计算面临的挑战

1）隔离 TEE 的特权软件

现有基于TrustZone TEE的特权软件通常具有很高的权限，只能被信任无法被隔离，机密计算需要隔离包括 TEE 特权软件或固件对于任务占用存储的访问，这样可以提供更高的安全等级。目前在众多用例和实例中，工作负载部署到易受攻击的公共云或边缘设备上，在这种情况下，机密计算环境需要确保 REE 和 TEE 中的其他固件 / 软件无法访问它，实现安全域隔离保证。

2）动态安全内存分配

机密计算某些任务会占用大量安全内存，如果无法支持动态安全内存分配会导致必须预留大量内存，导致成本效率问题。现在基于 TrustZone 的 TEE 无法支持动态安全内存分配，需要预留大量固定内存用于机密计算任务需要，因此如何动态安全内存分配是一项关键技术挑战。目前部署机密计算工作负载的方式主要有三种：基于 API/ 服务、基于安全的应用程序、基于容器或虚拟机。在后两种情况下，动态内存分配可以支持非常大的工作负载。

3.2.3 产业链协同使能

随着计算产业进入新一轮爆发浪潮，机密计算的安全战略支撑作用逐渐凸显，从培育期迈入关键的深耕期，在此背景下，机密计算产业链协同尤为重要。机密计算产业不是靠一家企业、一个公司就能完成的，机密计算将依托绿色计算产业联盟，构建从‘芯’到‘云’的能力，聚合生态之力，更好地服务企业用户。

对于机密计算产业需要从不同层面、不同角度来看待。具体来说，机密计算自下而上，产业可以分为绿色计算产业联盟、硬件、开源项目、产品四大层级（如图 5 所示），不同层级对应不同的需求端。其中，在绿色计算产业联盟层，主要依托联盟的白金会员、黄金会员、白银会员、普通会员一起，整合各个会员的产品链、价值链、资产链，优化流程，扩大机密计算的应用场景。在硬件层，基于芯片构建统一的机密计算安全生态，提供硬件安全能力的延伸，引领和发展生态，使能第三方进行 enclave 开发，北向建立硬件透明的统一软件开发接口。在开源项目层，可以通过社区开源开发者 SDK 与 TA 开发工具与文档、安全应用的 demo，如远程证明、TA 迁移等，以简化应用开发，使能客户安全集成机密计算功能。

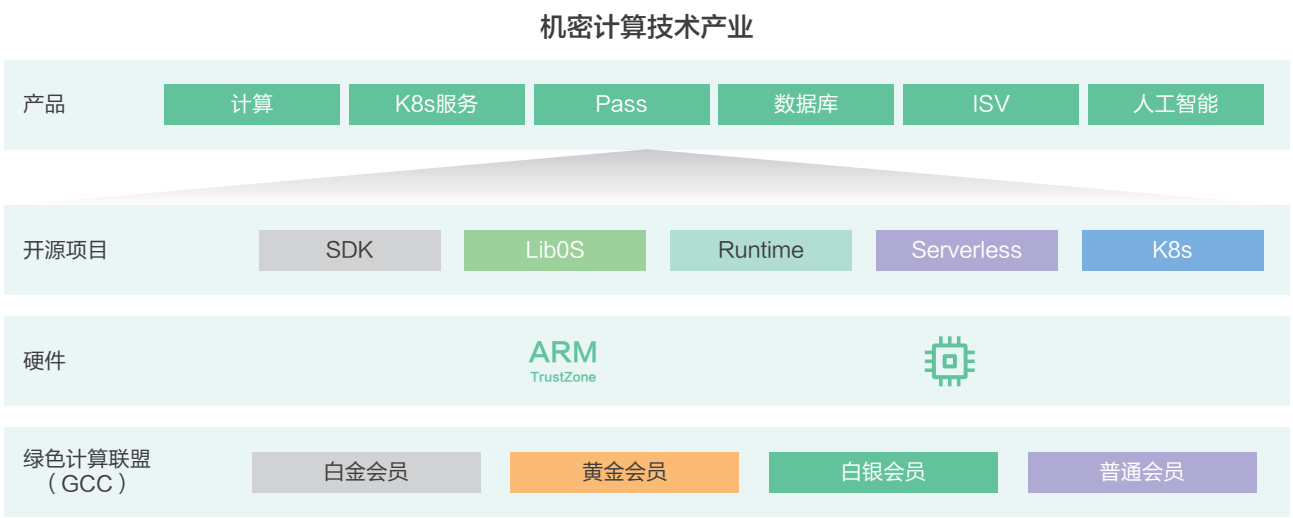


图 5 机密计算上下游产业链图

机密计算技术产业中，产品层具体解决用户的安全需求，通过全要素、全产业链、全价值的连接，提供安全产品和服务，包括计算服务、k8s 服务、Paas 服务、数据库产品、ISV 产品、AI 产品等，帮助用户实现安全透明的计算。其中 ISV 客户更多关注是可信应用的开发部署的便利性，以及平台基于场景的通用基础安全能力的实现，如通用加解密、远程证明、安全存储、基于硬件可信根的密钥派生等安全特性。

通过上述机密计算产业链分层次划分，机密计算参与方、协调方、用户等各类角色都能够找到自己的位置，上下游产业协同，并通过机密计算安全融合解决方案，打通供需两侧，完整覆盖不同层级的关键安全需求。

04 机密计算相关标准

4.1 可信执行环境

目前基于可信执行环境的机密计算的开发可以从任务处理能力、环境验证、通信安全、计算机密性、一致性、数据存储、审计等角度对产品能力提出统一要求。机密计算相关的标准包括可信执行环境、可信计算、联邦学习和多方安全计算等，机密计算也可以与这些技术实现融合。

可信执行环境（Trusted Execution Environment，缩写为 TEE）是数据计算平台上由软硬件方法构建的一个安全区域，可保证在安全区域内部加载的代码和数据在机密性和完整性方面得到保护。Global Platform（GP）已经发布了可信执行环境（TEE）、安全元件（SE）等系列标准。Global Platform 是一个由 100 多家成员公司推动的非营利性行业协会，成员们共同的目标是开发 Global Platform 的规范。这些规范现已被广泛认定为推动数字服务和设备在整个生命周期内受到信任并安全管理的国际标准。

Global Platform 通过制定标准和认证来保护数字服务，这有助于服务提供商和设备制造商之间的协作，使他们能够确保所有设备足够安全，能够防范威胁。GP 发布的标准主要有：

1. SE 管理：作为 GP 标准重要一项，有完善的 API、测试套件。
2. TEE API 规范：主要是 TEE 方案商和 TA 开发者必备的案头参考手册。
3. TEE 一致性规范：主要还包含测试相关。
4. TEE 管理框架：就是应用管理相关，也是需要各大 TEE 厂商所重视的。
5. TEE PP：也就是 TEE 的安全轮廓，是 TEE 安全认证的最重要的文档。

全国信息技术安全标准化技术委员会（TC260）已发布可信计算规范等系列标准，并正在制定 TEE 相关标准：《信息安全技术 可信执行环境系统架构》、《信息安全技术 可信执行环境服务规范》。

《信息安全技术 可信执行环境系统架构》规范了可信执行环境整体技术架构、硬件要求、安全启动过程基本要求、可信虚拟化、可信操作系统、可信应用与服务管理基本要求、可信服务基本功能及要求、跨平台应用中间件、可信应用基本要求等。本标准适用于智能手机、平板、行业终端等需要可信执行环境进行安全防护的领域。

《信息安全技术 可信执行环境服务规范》通过建立统一的可信服务安全框架，并对基于该框架的可信设备鉴别、可信人机交互、可信二维码、可信时钟以及可信位置等可信服务的功能和安全性进行有效定义和规范，统一可信服务的功能和安全服务及调用接口。本标准的使用者包括设备制造商、系统软件提供商、检测机构和科研机构等。

4.2 可信计算

可信计算（Trusted Computing）是世界网络安全的主流技术，TCG（Trusted Computing Group）于 2003 年正式成立，已有 190 多成员，以 WINDOWS 10 为代表可信计算已成焦点。国际的 TCG 标准从软件 (TPM1.2/2.0) 到硬件 (DICE)，全面定义计算、存储、网络等基础设施安全标准规范，强调兼容统一。TCG 标准系列包括可信平台模块 TPM、TPM 软件协议栈 TSS、可信网络连接 TNC、存储规范、移动规范、硬件完整性 DICE、PC 规范、IoT 规范等。可信计算 1.0 以世界容错组织为代表，主要特征是主机可靠性，通过容错算法、故障诊查实现计算机部件的冗余备份和故障切换。可信计算 2.0 以 TCG 为代表，主要特征是 PC 节点安全性，通过主程序调用外部挂接的 TPM 芯片实现被动度量。

信息安全标准化技术委员会 TC260 制定了 TCM 系列国家标准，从引入 TPM 标准逐渐转向自主可控背景下推出新的 TPCM 标准，TCM1.0 引入 TPM1.2，TCM2.0 贡献 TPM2.0，TPCM 标准推出主动度量新技术。等级保护 2.0 标准体系全面采用了具备主动免疫的可信计算 3.0 技术架构（TPCM\TCM），针对不同等级的安全要求，在计算环境、区域边界、通信网络、安全管理中心的各计算节点上实现了不同完备程度的信任传递。等级保护系列标准中一个显著的变化就是强化了可信计算技术使用的要求，把可信验证列入各个级别并逐级提出各个环节的主要可信验证要求。

信安标委 TC260 目前正在修订 TCM 标准 GB/T 29829—2013《信息安全技术　可信计算密码支撑平台功能与接口规范》，本标准描述可信计算密码支撑平台功能与接口规范的技术原理与要求，并详细定义了可信计算密码支撑平台的密钥管理、证书管理、密码服务等。本标准适用于可信计算密码支撑平台相关产品的研制、审查、测评与应用开发。

信安标委 TC260 正在制定 TPCM 标准《信息安全技术 可信计算规范 可信平台控制模块》，本标准描述了可信平台控制模块在可信计算平台双体系框架中的位置和作用，规定了基于可信平台控制模块的可信验证功能流程以及可信平台控制模块的功能组成、功能接口、安全防护和运行维护要求。本标准适用于指导可信平台控制模块的设计、生产和测评。

我国的可信计算 3.0 的主要特征是系统免疫性，其保护对象为系统节点为中心的网络动态链，构成“宿主 + 可信”双节点可信免疫架构，宿主机运算同时可信机进行安全监控，实现对网络信息系统的主动免疫防护 [5-6]。可信计算 3.0 其理论基础为基于密码的计算复杂性理论以及可信验证。它针对已知流程的应用系统，根据系统的安全需求，通过“量体裁衣”的方式，针对应用和流程制定策略来适应实际安全需要，为重要生产信息系统提供安全保障。

4.3 隐私计算

目前提供数据隐私保护的隐私计算技术包括多方安全计算、联邦学习、零知识证明、同态加密等多种方案或基础技术，在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算，主要相关的标准如下。

1）国际标准

ISO/IEC JTC1/SC27 已发布同态加密标准：ISO/IEC 18033-6:2019 IT Security techniques — Encryption algorithms — Part 6: Homomorphic encryption。本标准规范了同态加密的二种机制：指数 ElGamal 加密、Paillier 加密。针对每种机制，该标准规定了生成实体的参数和密钥、数据加密、数据解密、对加密数据同态操作等流程。本标准附录 A 定义了分配给本标准所述机制的对象标识符，附件 B 提供了数字实例。

ISO/IEC JTC1/SC27 正在制定多方计算标准：ISO/IEC NP 4922-1 Information security - Secure multiparty computation - Part 1: General。本标准规范了在数据保持机密的同时执行计算的加密机制以及它们的特性。本标准第 1 部分包含所有部分的共同定义和符号，特别是它定义了这些机制所涉及的处理过程、参与方和密码特性。

UN Global Working Group (GWG) on Big Data 已发布隐私计算手册《UN Handbook on Privacy-Preserving Computation Techniques》。本手册描述了统计分析敏感数据时保护隐私的动机、应用场景，描述了在保证隐私的同时分析敏感数据的技术，包括多方计算技术、同态加密、差分隐私、零知识证明、可信执行环境等。

IEEE 正在制定联邦机器学习标准 P3652.1 Federated Machine Learning Working Group “Guide For Architectural Framework And Application Of Federated Machine Learning”。联邦学习定义了一个机器学习框架，它允许在分布的数据所有者之间构建数据收集模型。本标准为跨组织的数据使用和模型构建提供了参考，同时满足适用的隐私、安全和监管要求。它定义了联邦机器学习的架构框架和应用指南，包括：a) 联邦学习的描述和定义；b) 联邦学习的类型和每种类型适用的应用场景；c) 联邦学习的性能评估；d) 相关的监管要求。

2）国内标准

中国通信标准化协会 (CCSA) TC601 发布了《基于多方安全计算的数据流通产品技术要求与测试方法》(修订版)、《基于可信执行环境的数据计算平台技术要求与测试方法》和《基于联邦学习的数据流通产品技术要求与测试方法》等标准，目前正在制定《基于区块链的隐私计算平台技术要求与测试方法》联盟标准。

《基于多方安全计算的数据流通产品技术要求与测试方法》标准于 2019 年 6 月首次发布。2020 年 6 月，项目组对标准进行了第一次修订，增加了多方安全容错性、升级支持等新的测试用例，提升了必选测试项的数量，也对原有测试用例进行了精简合并。本标准规范了利用安全多方计算技术实现数据的发布、跨组织流动等，从供应方到需求方传递过程中，对数据安全性进行保护，最终达到在任意参与方无法得到计算结果除外的其他方数据的情况下完成多方协同计算。

《基于可信执行环境的数据计算平台技术要求与测试方法》标准提出了基于可信执行环境的数据计算平台的建设目标和架构体系，从任务处理能力、算法拓展性、环境验证、通信安全、计算机密性、一致性、数据存储、审计和运维等九个角度对产品能力提出规范要求。

《基于联邦学习的数据流通产品技术要求与测试方法》标准明确了联邦学习的技术概念和架构视图，并从调度管理能力、数据处理能力、算法实现、效果及性能和安全性等五个方面对基于联邦学习的数据流通产品的能力提出建设规范。

《基于区块链的隐私计算平台技术要求与测试方法》标准聚焦于基于区块链技术所构建的隐私计算技术工具，该工具适用于保护数据隐私的协作计算应用场景，能够结合区块链技术保障数据计算的隐私、安全、可追溯和可扩展，保障交易数据端到端及全生命周期的隐私安全，为隐私计算建立完整的技术规范，助力数据流通行业的健康发展。

由中国信息通信研究院、中国移动通信集团有限公司牵头的《基于可信执行环境的安全计算系统技术框架》行业标准制定工作已于 2019 年 12 月成功立项启动。本标准定义了基于可信执行环境的安全计算系统的技术框架，来规范化基于可信执行环境的安全计算系统的定义、技术架构、技术特性、安全要求等。本标准适用于指导基于可信执行环境的安全计算系统的设计、开发、测试、运维等。

05 典型的机密计算应用场景

机密计算应用场景非常广泛，常见的应用有基于 TEE 技术对指纹保护、知识产权保护、AI 模型保护、多方计算与机密计算技术结合解决数据提供方的互信问题等等。其他如区块链隐私计算、区块链 +AI、隐私边缘计算等都可以构建在机密计算技术基础上，以更好的服务应用场景。业务场景与机密计算技术的结合能力是构建机密计算产业联盟的关键

5.1 区块链场景下的典型解决方案

区块链场景下的典型安全解决方案将利用机密计算、区块链等技术解决数据隐私问题，针对密钥以及当前物理加密机性能不足，希望基于硬件构建隐私保护的密钥管理系统，提高性能。该方案由区块链、安全、大数据等多种技术结合而成，能够提供一站式企业级可信数据协作解决方案，力图解决目前在数据协作过程中遇到的难题。

该方案具有技术创新领先、支持用户根据场景灵活选择、生态开放三大特点。在该方案中，智能云区块链平台提供了基于区块链的数据和计算过程的全流程监测、溯源和智能合约能力，同时结合机密计算安全硬件设备和技术，提供了区块链链外的可信计算能力，保障了数据在链外存储和链外运算过程中的安全、隐私、可信和公平。

其中，机密计算安全软件开发套件，能够帮助应用程序开发人员更好的保护选定的代码和数据，免遭在硬件层的泄露或修改，机密计算安全技术保障了内存计算、加密通信和安全，还提供了侧信道攻击的防御能力。

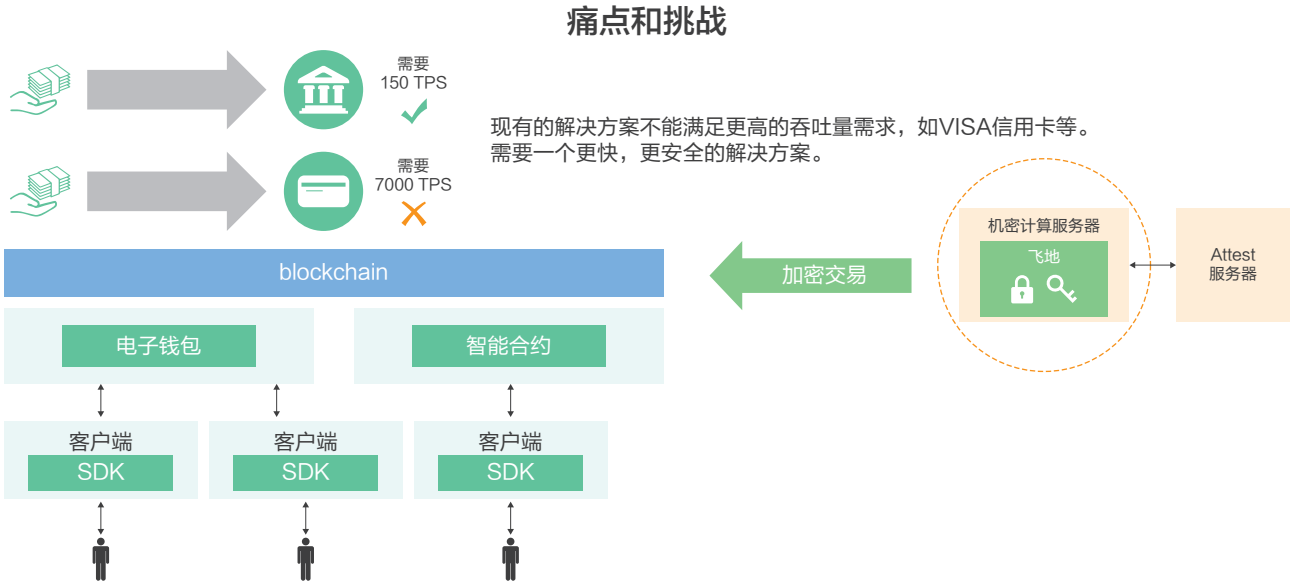


图 6 区块链安全加密交易保护图

同时该解决方案保持了开放性，兼容多方安全计算 MPC、可信执行环境 TEE、零知识证明等多种技术，为企业用户提供了不同需求等级的方案选择。

区块链场景下的机密计算安全可以开拓更多的应用场景和落地解决方案，并推广至金融、智慧城市等行业用户，让更多行业和组织享受到信息的自由流动，推动千行万业智能化升级。

5.2 AI 场景下的典型解决方案

训练数据以及模型的保密是当前业务痛点，很多企业不愿意把数据交给用户训练。由于对外部署的 AI 模型携带大量知识产权，一旦被逆向或泄露，既会对技术护城河造成破坏，也会降低对抗性样本攻击的难度，导致安全问题，这是 AI 场景下目前存在的普遍问题与挑战。

应对这种威胁的一种方案是，使用方把 AI 模型和训练 / 预测数据加密存储，只有在使用时才将其输入 Enclave，在 Enclave 里面解密，由 Enclave 中运行的 AI 框架处理，结果根据具体场景需求以明文返回或加密返回并在使用方本地解密。这要求 Enclave 能支持常见的 AI 框架，例如 Tensorflow、PyTorch、Mindspore，而要做到这一点极为挑战——一方面是因为这些 AI 框架一般使用了复杂的多线程等性能优化的运行环境，另一方面是因为 Enclave 又偏偏难以提供这些支撑环境。

AI 场景下的机密计算框架支撑上层业界通用的、以及自研的 AI 框架，AI 应用几乎零改动，机密计算的这种灵活性将让开发者完全发挥 TEE 的优点，可迅速移植应用，而不需要额外修改代码。上层 AI 应用灵活调用机密计算能力，可以较为轻松的高效运行常见 的 AI 框架。

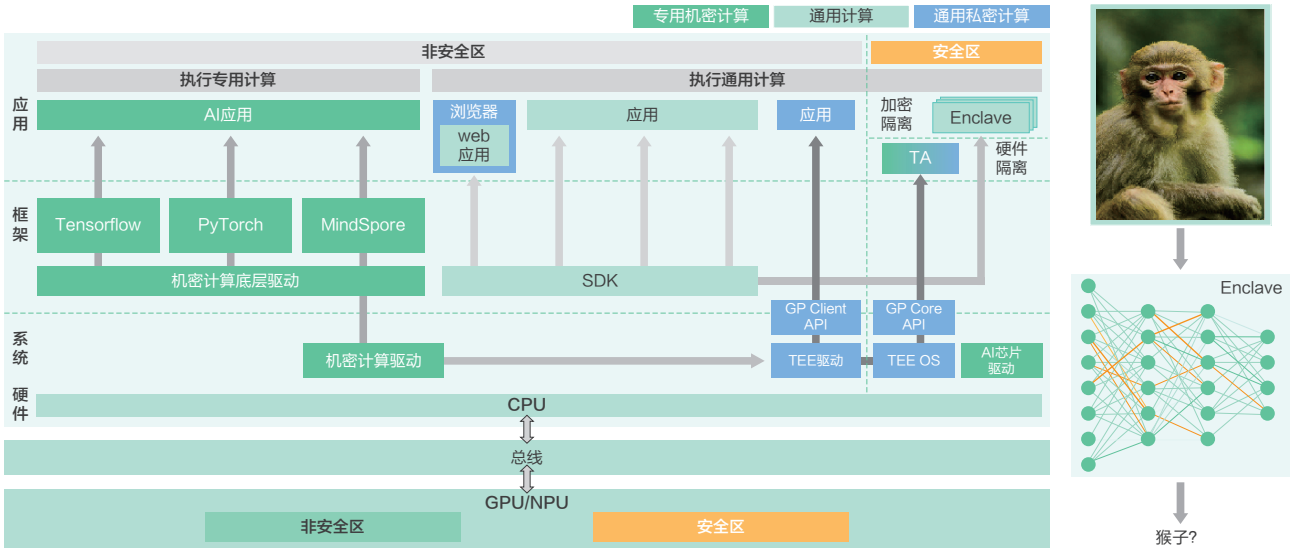


图 7 AI 模型安全保护图

5.3 政务数据融合场景下的典型案例

2015 年，国务院印发的《促进大数据发展行动纲要》中提到，在开放前提下加强安全和隐私保护，在数据开放的思路上增量先行，提出建成国家统一的数据开放平台。因此，政府数据融合打通，是对政府数据开放共享政策的落实。如何数据公开、控制数据风险、保障隐私合规、提升数据价值成为政府急需解决的问题。

2018 年，为深化各级公共资源交易平台互联互通，促进公共资源交易数据汇聚共享，国家发展改革委、财政部、自然资源部、国资委近日联合公布《公共资源交易平台系统数据规范（V2.0）》（发改办法规［2018］1156 号），定义了公共资源交易的统一交易标识码编码规则，明确了公共资源交易的分类原则与类目，规定了工程建设项目招标投标、政府采购、土地使用权出让、矿业权出让、国有产权交易等领域交换共享数据的数据格式要求，同时为碳排放权、排污权、林权、药品和二类疫苗等交易领域的交易数据交换共享做了衔接。在国家政策的积极推动、地方政府和产业界的带动下，贵州、武汉等地开始率先探索大数据交易机制，我国已有近 20 个地方政府陆续推出数据开放平台。

政务大数据蕴含着巨大的经济与社会价值，其开放与共享对于促进政府自身转型、社会需求获取模式转型、打造智慧城市以及产业经济转型都具有重要意义。当前我国政务大数据开放与共享的障碍还有很多，除了相关法律法规较为滞后等因素外，数据安全共享技术也是制约因素之一。

传统的数据流通方案往往是将原始数据直接进行明文传输交易或线下交易，并未充分考虑数据安全和隐私安全问题。然后由于缺乏可信数据交易服务的相关技术方案，在大数据交易的过程中无法有效地保障“数据确权”和“隐私保护”等问题，企业参与大数据交易的意愿不强，交易方式方案有可能导致的违法风险，将逐渐被越来越严格的隐私保护相关法规所禁止。

AI 时代最关键的生产要素是“数据、算法和算力”，产品能将数据、算法与算力分离，使得算法和数据能够安全进入大数据交易中心执行可信流通。能够让更多专业的公司或团队贡献数据资源或从事算法研发，构建良好的数据生态，不断地为大数据交易中心注入活力。

企业信用在招投标、政府采购、吸引人才等商业活动中起着至关重要的作用。如果将企业的经营发展形势、财务状况、知识产权、网络舆情等国家权威数据、开源网络数据、商业数据进行流通共享，可以获得企业信用等级。通过将企业名录、政府招投标数据、商标数据、违法犯罪数据、企业年报数据、专利数据等多方企业数据进行虚拟融合，对企业信用进行综合评价。

在政务数据开放共享的过程中，由于缺乏可信的数据资产权利确认方案，导致政府部门不愿意共享数据。因缺乏有效的隐私安全保护技术，数据共享后无法限制数据用途，导致数据滥用和隐私泄露等问题，政府部门也不敢共享数据。机密计算解决方案产品可以与大数据开发组件集成，打破政府部门数据孤岛，实现跨部门与社会数据等安全共享。

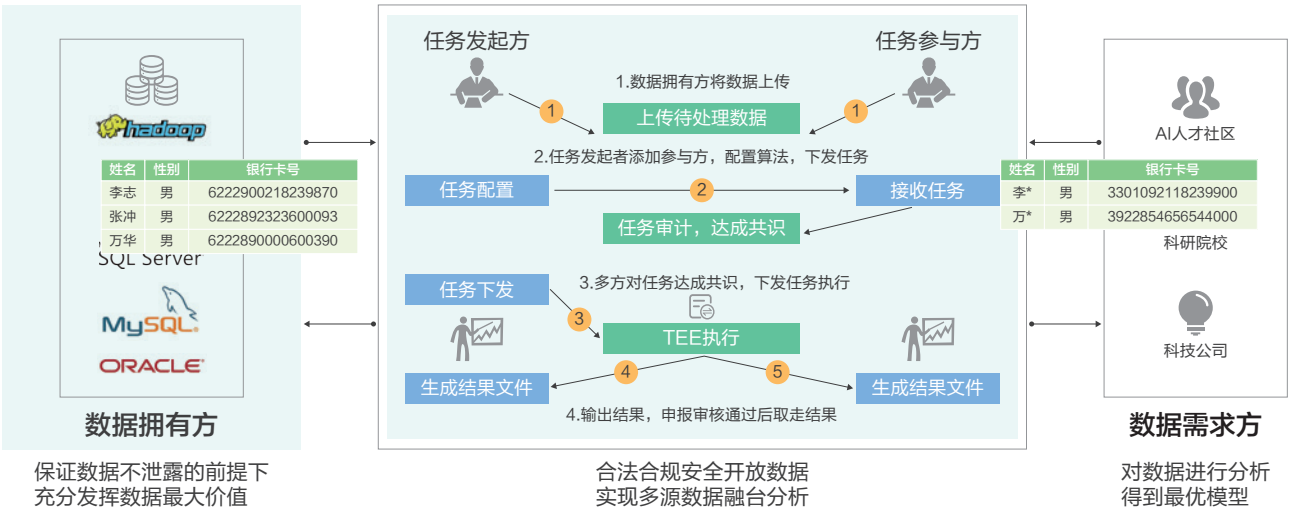


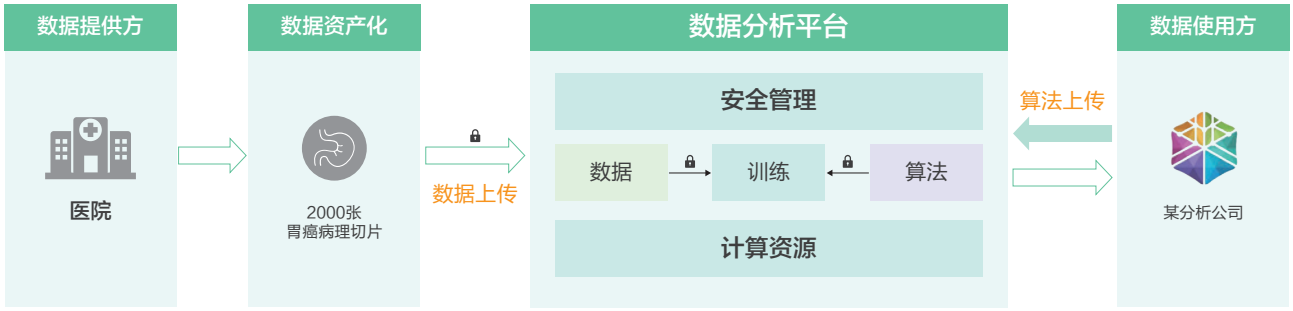
图 8 政务数据安全融合平台图

5.4 医疗数据共享场景下的典型案例

医疗数据包含患者信息、用户资料、基因数据等大量个人隐私数据，导致医疗机构、保险、药企、医药设备厂商之间数据流通共享难以高效协同，医疗数据价值难以有效发挥。机密计算可以为医疗数据参与方建立安全数据流通基础设施，推动医疗数据价值最大化利用。

目前各地卫健委响应国家健康医疗大数据战略纷纷建设医疗大数据平台，其医疗数据成为一座亟待挖掘的金矿。但碍于数据安全性考虑，医疗机构等多保持审慎的态度，对于与第三方企业共享数据积极性不足。医疗机构可基于机密计算数据安全开放平台实现健康医疗大数据的安全共享，在保证数据可用不可见，原始数据不流出的情况下，提供给医院或第三方企业对医疗数据进行充分挖掘。

基于机密计算的安全计算平台，可以建立医疗数据安全共享科研平台，合法合规安全可控地向医院医生、科研机构、药企等单位开放医疗数据，提供丰富的算法与建模工具降低医生数据分析门槛，充分挖掘医疗数据价值。



数据拥有者担心的安全问题：
1.数据提供方担心隐私医疗数据被非法泄露；
2.如何保障数据分析公司的算法知识产权问题

机密计算的结合点：A模型部害在 Enclave中，数据提供方将数据加密后上传，并确保只在特定的 Enclave中才会解密，完成相应的推理任务。这样数据的机密性以及模型的安全性都得到良好的保障

图 9　医疗数据安全开放共享科研平台图

医疗科研数据的开放共享，对医疗行业的赋能表现在多个方面，如辅助医生诊疗决策、提升患者就诊效率、帮助医药企业缩短新药研发的时间周期、节约新药研发的成本；在医保药械准入与定价方面，则能够精细化仿真和预测各种药械进入医保和不同定价给整个医疗系统和患者带来的变化，为更经济有效的医疗社会福利决策提供参考；此外，医疗大数据也可以帮助保险公司实现精准产品开发、风险控制。

5.5 互联网金融场景下的典型案例

金融行业需要对贷款申请、交易欺诈、老赖等风险建立完善风控机制。因此对银行、证券、保险、互联网金融公司等多方数据有很强的流通共享需求，但需应对数据泄露、个人隐私泄露等顾虑。通过融合多方数据，多方数据核实、多方联合建模，为多方联合风控提供安全数据流通解决方案。

例如，银行、借贷机构、保险机构、政府等风控多方可以联合各自的用户数据（姓名、身份证、年龄、借贷记录、信用记录），如果各方数据核实有用户重叠，说明重叠用户有多头借贷行为。

此外，机密计算在互联网金融联合建模如产品精算定价方面也有很好的安全解决方案。例如，机动车辆保险是中国财险市场中的“龙头险种”，业务份额一直盘踞着中国财险市场的大半河山。由于车险产品自身的特殊属性，费改以来车险产品的定价策略直接影响着保险机构的市场推广与企业收益。某保险机构希望能够通过自有业务数据，与某机构的数据进行融合训练、联合建模分析，提升已有精算定价模型 KS 值，从而为公司产品精算定价提供辅助决策。

由保险公司提供相关的赔付率、赔付金额，通过机密计算平台进行融合训练、建模分析，与某机构的数据进行融合训练，并将模型结果应用于车险精算模型。

该方案具有以下客户价值：

1）提供完备的数据安全及个人信息保护能力和业务机制

数据的使用通过“事前授权 - 事中监控 - 事后审计”进行严格的把控，同时对所有用户数据操作进行了全生命周期的日志记录，实现所有数据操作可追溯、可审计、可定责。帮助企业建立一套全流程的申报审核机制，严格保障数据安全。

2）提升产品精算定价模型区分度 KS 值

保障数据安全性及隐私性的前提下，由保险公司提供相关的赔付率、赔付金额，与其它机构的数据通过机密计算平台进行融合训练、建模分析，并将模型结果应用于车险精算模型，提升车险精算定价模型区分度 KS 值。具体提升效果如下图所示：

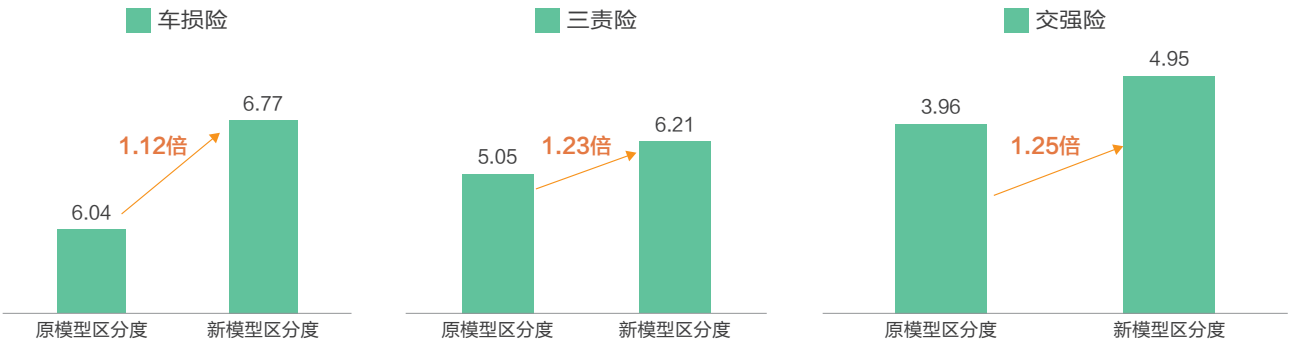


图 10 产品精算定价模型区分度 KS 值对比图

通过车险精算模型的优化，贷后表现良好，不良率低于业界水平均值 10%，同时该项目日均调用量达到 50W+，既为保险机构降低了风险，又节省了成本。

3）促进行业数据流通，提升数据变现能力

平台提升企业对数据全生命期的管理能力，促进企业内部和企业间的数据流通，提升数据变现能力，将赤裸裸的数据交易升级为数据服务，为拥有数据的企业实现最大化的数据挖掘价值。

附录 A：术语表

A.1 机密计算（Confidential Computing）

机密计算是通过在基于硬件的可信执行环境中执行计算来保护使用中的数据的一种技术。

A.2 隐私计算（Privacy-preserving Computation）

隐私计算（Privacy-preserving Computation，缩写为 PC）是指在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的信息技术。广义上是指面向隐私保护的计算系统与技术，涵盖数据的产生、存储、计算、应用、销毁等信息流程全过程，想要达成的效果是使数据在各个环节中“可用不可见”。隐私计算的常用技术方案有多方安全计算（Secure Multi-Party Computation）、联邦学习（Federated Learning）、零知识证明（Zero-Knowledge Proof）、同态加密（Homomorphic Encryption）等。

A.3 多方安全计算（Secure Multi-Party Computation）

多方安全计算（Secure Multi-Party Computation，缩写为 MPC 或 SMC）是指针对无可信第三方情况下，安全地进行多方协同的计算问题。即在一个分布式网络中，多个参与实体各自持有秘密输入，各方希望共同完成对某函数的计算，而要求每个参与实体除计算结果外均不能得到其他参与实体的任何输入信息。多方安全计算的常用技术有混淆电路 (Garbled Circuit)、不经意传输 (Oblivious Transfer)、秘密分享（也称为秘密分割，Secret Sharing）等。

A.4 联邦学习（Federated Learning）

联邦学习（Federated Learning，缩写为 FL）是一种多个参与方在保证各自原始私有数据不出数据方定义的私有边界的前提下，协作完成某项机器学习任务的机器学习模式。

A.5 可信执行环境（Trusted Execution Environment）

可信执行环境（Trusted Execution Environment，缩写为 TEE）是基于一定安全需求设计的硬件和软件的组合运行环境，为数据保护提供安全传输、存储和处理等基础服务，保证其上所运行软件的机密性、完整性。可信执行环境通常与富执行环境并存于同一设备，两个运行环境同时运行。

A.6 不经意传输（Oblivious Transfer）

不经意传输（Oblivious Transfer，缩写为 OT）是数据计算平台上由软硬件方法构建的一个安全区域，可保证在安全区域内部加载的代码和数据在机密性和完整性方面得到保护。不经意传输是一种可保护隐私的双方通信协议，它允许发送方以一种保护双方安全的方式将信息发送给接收方，发送方并不知道接收方接收的是哪份信息，且也不会泄露除接收方接收信息之外的其他信息。

A.7 零知识证明（Zero-Knowledge Proof）

零知识证明（Zero-Knowledge Proof，缩写为 ZKP）是一种涉及两方或更多方的协议，证明者向 验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。

A.8 同态加密（Homomorphic Encryption）

同态加密（Homomorphic Encryption，缩写为 HE）是一种隐私保护技术，提供了一种对加密数据进行处理的功能，但是处理过程不会泄露任何原始内容。在针对相同明文分别进行明文运算与密文计算中，能够保证密文计算结果的解密值与明文运算结果一致。

附录 B：缩略语表

英文缩写	英文全称	中文全称
CA	Client Application	客户端应用
CCC	Confidential Computing Consortium	机密计算联盟
CSP	Cloud Service Provider	云服务提供商
FL	Federated Learning	联邦学习
GDPR	General Data Protection Regulation	通用数据保护条例
GP	Global Platform	全球平台国际标准组织
HE	Homomorphic Encryption	同态加密
ISV	Independent Software Vendors	独立软件供应商
MPC	Multi-Party Computation	多方计算
OT	Oblivious Transfer	不经意传输
PC	Privacy-Preserving Computation	隐私计算
POSIX	Portable Operating System Interface	可移植操作系统接口
REE	Rich Execution Environment	富执行环境
SE	Secure Element	安全元件
SEV	Secure Encrypted Virtualization	安全加密虚拟化
SGX	Software Guard Extensions	软件保护扩展
TA	Trusted Application	可信应用
TCM	Trusted Cryptography Module	可信密码模块
TEE	Trusted Execution Environment	可信执行环境
TMF	TEE Management Framework	TEE 管理框架
TPCM	Trusted Platform Control Module	可信平台控制模块
TPM	Trusted Platform Module	可信平台模块
VSM	Virtual Secure Mode	虚拟安全模式
ZKP	Zero-Knowledge Proof	零知识证明

附录 C：参考文献

1. Confidential Computing Consortium, Confidential Computing: Hardware-Based Trusted Execution for Applications and Data, July 2020.
2. Gartner, Inc., How to Make Cloud More Secure Than Your Own Data Center, Neil MacDonald and Tom Croll, 9 October 2019.
3. Confidential Computing Consortium, Confidential Computing Deep Dive v1.0, October 2020.
4. 百度安全，MesaTEE 通用安全计算平台解决方案，2020-08.
5. 沈昌祥，主动免疫可信计算筑牢网络空间安全，https://www.secrss.com/articles /10433，2018-11.
6. 国家标准《信息安全技术 可信计算规范 可信平台控制模块》(送审稿)，2020-05.
7. CCSA TC601 联盟标准《基于区块链的隐私计算平台技术要求与测试方法》，2020-05.

绿色计算产业联盟

地址：北京市东城区安定门东大街 1 号
邮编：100007
网址：http://www.opengcc.org
邮箱：liyang@opengcc.org
电话：010-68208678